TP1
Analyse du trafic réseau

1 Objectif

Se familiariser avec les outils de capture du trafic et pouvoir faire l'analyse.

2 Les outils

2.1 TCPdump

Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression[1].

2.2 Wireshark

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions[2].

2.3 Nmap

Nmap est un scanner de ports open source créé par Fyodor et distribué par Insecure.org. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant[3].

3 Plateforme du TP

Pour la réalisation de ce tp, on va adopter la plateforme illustrée au schéma suivant:

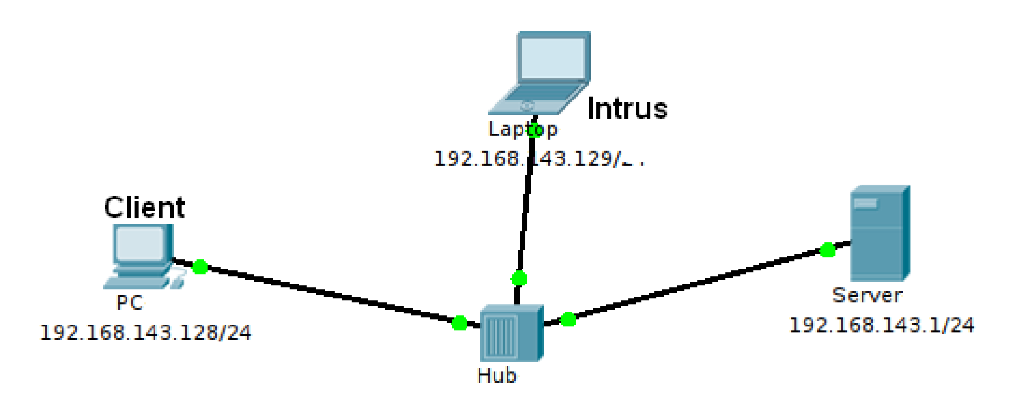


Figure 1: Réseau LAN

4 Capture du trafic avec TCPdump

Toute les commandes suivantes doivent être lancées en mode **root**.

[1] man tcpdump
[2] http://www.wireshark.org/about.html
[3] Wikipédia

4.1 Visualisation du trafic avec TCPdump

1 Sur la machine intrus, lancez la commande *tcpdump*

2 Faites un ping depuis le poste du client vers le serveur

3 Ctrl + c pour mettre fin à la capture

4 Visualisation de la capture

4.2 Analyse de l'en-tête Ethernet

1 *arp -d* pour effacer le cache ARP du poste Client

2 Afficher en hexadécimal (option -x) les trames icmp échangées entre le client et le serveur

3 Une commande complète: tcpdump -x -X -s 0 src host 192.168.143.131 and dst host 192.168.143.128 and icmp

À la dernière commande, nous avons capturé les paquets transitant de la machine 192.168.143.131 vers la machine 192.168.143.128. Ces paquets seront affichés au format hexadécimal et ascii (-x -X) quelle que soit leur taille (-s 0).

4.3 Analyse de l'entête TCP/IP

1 Effectuer une demande de connexion *ftp* depuis win xp vers ubuntu

2 Capturer ce trafic et analyser le login et le mot de passe

3 Faites l'inverse mais avec le service telnet (pensez à lancer le service depuis les services des outils d'administration)

5 Capture du trafic avec Wireshark

Reprendre le TP mais en utilisant le Wireshark cette fois.

5.1 Filtrage de capture

Capture ⟶ Option ⟶ Capture filter :

- tcp dst port 3128
- ip src host 10.1.1.1
- host 10.1.2.3
- src portrange 2000-2500
- not imcp
- src host 10.7.2.12 and not dst net 10.200.0.0/16

5.2 Filtrage d'affichage

Durant la capture, le champs *filter*

- snmp || dns || icmp
- ip.addr == 10.1.1.1
- ip.src != 10.1.2.3 or ip.dst != 10.4.5.6
- ip.src != 10.1.2.3 and ip.dst != 10.4.5.6
- tcp.port == 25
- tcp.dstport == 25

6 Nmap

Aux prochaines étapes, pensez à surveiller le comportement de nmap en utilisant le wireshark par exemple.

- Sur le poste "intrus", faites un scan pour détecter les machines actives de votre réseau (option -sP).
- Choisissez une machine et détecter ses ports ouverts (option option -sS)
- Déterminez le système d'exploitation de la machine cible (option -O)